UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NORTH DAKOTA

Stacy Kolkind, individually and on behalf of all others similarly situated, Plaintiff, vs. DMS Health Technologies, Defendant.	Case No. 3:23-cv-204 **ORDER**

Constance Boyd, individually and on behalf of all others similarly situated, Plaintiff, vs. DMS Health Technologies, Defendant.	Case No. 3:23-cv-212 **ORDER**

In this consolidated putative class action, plaintiffs allege defendant DMS Health Technologies (DMS) failed to adequately safeguard plaintiffs' protected health information (PHI) and personally identifying information (PII), resulting in a data breach that caused harm to plaintiffs. Plaintiffs Stacy Kolkind and Constance Boyd, on behalf of themselves and all others similarly situated, filed an amended consolidated class action complaint (hereinafter, amended complaint) against DMS[1]. (Doc. 36). DMS

[1] On October 17, 2023, Kolkind filed a complaint against DMS. Kolkind v. DMS Health Tech., No. 3:23-cv-204, Doc. 1 (D.N.D. Oct. 17, 2023). On October 30, 2023, Boyd filed a complaint against DMS. Boyd v. DMS Health Tech., No. 3:23-cv-212, Doc. 1 (D.N.D. Oct. 30, 2023). Kolkind and Boyd later moved to consolidate the two cases, and this court granted the motions. Kolkind, No. 3:23-cv-204 at Docs. 5, 23; Boyd, No. 3:23-

filed a motion to dismiss plaintiffs' amended complaint under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). (Doc. 42). Plaintiffs filed a response in opposition to the motion, and DMS filed a reply. (Doc. 46; Doc. 47). The court held argument on the motion on March 14, 2025.

Factual Background

The factual background described below, which is accepted as true for purposes of this motion, is taken from plaintiffs' amended complaint. (Doc. 36). DMS is a business that provides imaging services to various healthcare companies. During its work with healthcare companies, DMS "acquired, collected, and stored" private information, including patients' names, patients' dates of birth, the type and date of exams or services patients received, and the attending physicians' names. Id. at 1-2. Plaintiffs claim they received medical services from healthcare companies that utilized DMS's services and DMS's network consequently stored their PHI and PII (hereinafter collectively, private information).

Plaintiffs allege DMS provided notice that its systems had been breached. Kolkind alleges she received a notice dated September 25, 2023, and Boyd alleges she received a notice dated October 17, 2023. Plaintiffs allege,

> According to DMS's notice, on April 23, 2023, DMS became aware of suspicious activity related to certain computer systems and determined that there was unauthorized access to DMS's network between March 27 and April 24, 2023, and the unauthorized actor had the ability to access certain information stored on the network during the period of access.
>
> On no later than April 24, 2023, upon information and belief, unauthorized third-party cybercriminals gained access to Plaintiffs['] and Class Members'

cv-212 at Docs. 7, 18. On March 25, 2024, plaintiffs filed a consolidated complaint. Kolkind, No. 3:23-cv-204 at Doc. 26. DMS moved to dismiss, (Doc. 29), but the parties then stipulated to plaintiffs filing an amended complaint in response to the motion to dismiss, (Doc. 34).

> Private Information as hosted with Defendant, with the intent of engaging in the misuse of the Private Information, including marketing and selling Plaintiffs[’] and Class Members’ Private Information.

Id. at 2, 18, 20.

Kolkind alleges around April 22, 2023, a hacker gained access to her email account. Immediately thereafter, she noticed several unauthorized transactions on a prepaid card totaling at least $190, and an unauthorized redemption of a $200 Southwest Airlines voucher. She also alleges loss of time and money monitoring and mitigating harm from the breach. Id. at 18-20. Boyd solely alleges loss of time and money monitoring and mitigating harm from the breach. Id. at 20-21.

Plaintiffs bring claims for declaratory relief, negligence, breach of an implied contract, breach of an implied covenant of good faith and fair dealing, unjust enrichment, breach of a third-party beneficiary contract, invasion of privacy, and unauthorized disclosure of private information in violation of North Dakota Century Code section 51-22-02. DMS moves to dismiss all claims under Rules 12(b)(1) and 12(b)(6), alleging plaintiffs lack standing and the amended complaint states no claim upon which relief could be granted.

Law and Discussion

1. Motion to Dismiss Under Rule 12(b)(1)

DMS moves to dismiss plaintiffs’ claims under Rule 12(b)(1) for lack of subject matter jurisdiction, asserting plaintiffs lack standing to bring their claims. Jurisdiction is a threshold question that must be decided at the outset of a case. Green Acres Enters., Inc. v. United States, 418 F.3d 852, 856 (8th Cir. 2005) (citing Osborn v. United States, 918 F.2d 724, 729 (8th Cir. 1990)). In deciding a motion challenging jurisdiction under Rule 12(b)(1), a court “must distinguish between a facial attack—where it looks only to

the face of the pleadings—and a factual attack—where it may consider matters outside the pleadings." Croyle v. United States, 908 F.3d 377, 380 (8th Cir. 2018). A facial attack asserts the complaint does not allege facts supporting subject matter jurisdiction. Davis v. Anthony, Inc., 886 F.3d 674, 679 (8th Cir. 2018). A factual attack challenges the veracity of the facts alleged in support of subject matter jurisdiction. Id. Here, DMS raises a facial attack, so the court considers the factual allegations of the complaint as true and construes all reasonable inferences in plaintiffs' favor. See Carlsen v. GameStop, Inc., 833 F.3d 903, 908 (8th Cir. 2016); Branson Label, Inc. v. City of Branson, Mo., 793 F.3d 910, 914 (8th Cir. 2015).

To invoke federal court subject matter jurisdiction, a plaintiff must establish three elements of Article III standing. First, there must be an injury in fact, which is "an invasion of a legally-protected interest which is (a) concrete and particularized and (b) actual and imminent, not conjectural or hypothetical." Sierra Club v. Robertson, 28 F.3d 753, 758 (8th Cir. 1994). Second, "there must be a causal connection between the injury and conduct complained of" meaning the injury must be "fairly traceable to the challenged action of the defendant." Id. Third, "it must be likely as opposed to merely speculative that the injury will be redressed by a favorable decision." Id. This case is at the pleading stage, where plaintiffs must "clearly allege facts" demonstrating the elements of standing. In re SuperValu, Inc., 870 F.3d 763, 768 (8th Cir. 2017) (quoting Spokeo, Inc. v. Robins, 578 U.S. 330, 338 (2016)); see also Sch. of the Ozarks, Inc. v. Biden, 41 F.4th 992, 997 (8th Cir. 2022) ("At the pleading stage, therefore, a plaintiff must 'allege sufficient facts to support a reasonable inference that [it] can satisfy the elements of standing.'") (quoting Animal Legal Def. Fund v. Vaught, 8 F.4th 714, 718 (8th Cir. 2021)).

Regarding Article III standing, DMS claims Kolkind lacks standing to bring any common law or statutory claims because her alleged injuries of a hacked email account, unauthorized use of a prepaid card, and unauthorized use of an airline voucher are not injuries in fact that are fairly traceable to any action of DMS. DMS also contends both named plaintiffs' alleged injuries of loss of time and money monitoring and mitigating harm from the breach do not constitute injuries in fact and are not fairly traceable to DMS's actions. Lastly, DMS claims plaintiffs lack standing to bring a declaratory judgment claim because their alleged future injuries are abstract.

A. Injury in Fact

Plaintiffs allege a hacker accessed Kolkind's email account days after DMS's network was breached. Soon thereafter she noticed several unauthorized transactions on a prepaid card and unauthorized use of an airline voucher. "So long as the facts alleged in the complaint demonstrate [plaintiffs'] actual injury, plaintiffs have met their burden at the pleading stage." SuperValu, Inc., 870 F.3d at 772. In SuperValu, Inc., the court found an allegation that the plaintiff incurred a fraudulent charge on his credit card was sufficient to show an injury in fact. At this stage in the litigation, the court finds Kolkind's alleged injuries are concrete and particularized and therefore meet the injury in fact element of standing.

Both Kolkind and Boyd allege loss of time and money monitoring and mitigating harm from the data breach. Because the breach allowed access to their private information, plaintiffs allege they will continue to be at an increased risk of identity theft and fraud for years to come. Plaintiffs allege unauthorized third-party cybercriminals gained access to their private information with the intent of engaging in misuse of the information, including marketing and selling their private information.

In SuperValu, Inc., the Eighth Circuit found the plaintiffs' allegations of costs and time incurred to mitigate their risk of identity theft, review information about the breach, and monitor their account information did not constitute an injury in fact for purposes of standing because the plaintiffs did not allege a substantial risk of future identity theft. 870 F.3d at 771. Despite the plaintiffs' allegation their credit card information had been stolen, the court held theft alone did not create a substantial risk of future harm since the alleged stolen information did not include any PII and therefore, there was little to no risk of future identity theft. Thus, the plaintiffs' allegations were insufficient to support standing. 870 F.3d at 769-72.

A district court in Minnesota interpreted SuperValu, Inc. to "strongly suggest [ ] that substantial risk of future harm is sufficiently alleged when the stolen data includes PII." In re: Netgain Tech., LLC, No. 21-CV-1210, 2022 WL 1810606, at *5 (D. Minn. June 2, 2022). The Netgain Tech., LLC, court went on to state,

> Other circuits have held that there is a substantial risk of future harm when PII and PHI is stolen. For example, the Sixth Circuit has held that plaintiffs suffer a concrete harm when they allege a substantial risk of future harm arising from data theft. Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388–89 (6th Cir. 2016) (explaining that "it would be unreasonable to expect Plaintiffs to wait for actual misuse" where they already knew "that they have lost control of their data"). The Seventh and Ninth Circuits have reached the same conclusion. See, e.g., Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693-94 (7th Cir. 2015) (finding an injury in fact where plaintiffs alleged a substantial risk of future harm due to a data breach); Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (finding injury in fact where plaintiffs "alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data" and explaining that it would be different "if no laptop had been stolen"); but see Reilly v. Ceridian Corp., 664 F.3d 38, 40, 44 (3d Cir. 2011) (finding no risk of future harm because it was unknown "whether the hacker read, copied, or understood" the information, and there was "no evidence that the intrusion was intentional or malicious" or that a "taking occurred").

> This caselaw supports Plaintiffs' argument that they have adequately alleged a substantial risk of future harm in this case because their PII and PHI was stolen. See In re 21st Century Oncology Customer Data Sec. Breach Litig., 380 F. Supp. 3d 1243, 1253-54 (M.D. Fla. 2019) (analyzing the circuit split and explaining that the facts weigh in favor of finding an injury in fact where stolen information "includes personally identifiable information"). Like in Galaria, Remijas, and Krottner, Plaintiffs PII and PHI—sensitive data that was not stolen in SuperValu—is in the hands of ill-intentioned criminals, and Plaintiffs with credit took concrete steps to monitor their credit in response to the Data Breach. And unlike Reilly, there is no dispute that the criminals intentionally stole and sought to profit from Plaintiffs' Sensitive Information. As such, the Court finds that Plaintiffs have sufficiently plead a substantial risk of future harm.

2022 WL 1810606, at *5.

Like Netgain Tech., this case is distinguishable from SuperValu, Inc. because the data involved in the breach was different; this case and Netgain Tech. both involve PII and PHI—sensitive data that was not stolen in SuperValu, Inc. This court finds plaintiffs have clearly alleged facts demonstrating substantial risk of future harm sufficient to meet the injury in fact element of standing. Even assuming plaintiffs did not sufficiently allege future harm, Kolkind would meet the injury in fact element of standing because of the alleged harm she has already incurred. Boyd could also be considered to have met that element, since she is seeking the same relief as Kolkind. "Typically, if many plaintiffs seek the same relief and at least one of them has Article III standing, the court need not determine whether others also do." Morehouse Enters., LLC v. Bureau of Alcohol, Tobacco, Firearms & Explosives, 753 F. Supp. 3d 817, 826 n.3 (D.N.D. 2024) (quoting M.M.V. v. Garland, 1 F.4th 1100, 1110 (D.C. Cir. 2021)). A class action suit can proceed as long as one named plaintiff has standing. SuperValu Inc., 870 F.3d at 771.

B. Fairly Traceable to DMS's Actions

Plaintiffs claim DMS failed to adequately maintain security measures to prevent a data breach and the resulting exposure of their private information. According to the

complaint, DMS gave notice of a breach that occurred between March 27 and April 24, 2023, and during that time an unauthorized actor had the ability to access the private information stored on DMS's network. During the same time frame, Kolkind alleges a hacker gained access to her email account and soon thereafter she noticed several unauthorized transactions on a prepaid card and unauthorized use of an airline voucher.

The Eighth Circuit has held, "An injury is fairly traceable if the plaintiff shows a causal connection between the injury and the conduct complained of that is not the result of the independent action of some third party not before the court." SuperValu, Inc., 870 F.3d at 776 (internal quotations omitted). In SuperValu, Inc., the court found the plaintiff's allegations that the "[d]efendants failed to secure customer Card Information on their network, their network was subsequently hacked, customer Card Information was stolen by the hackers, and [the plaintiff] became the victim of identity theft after the data breaches" met the "relatively modest" burden at the pleading stage to show a causal connection between the injury and the defendant's actions. Id. at 772. The Eighth Circuit further stated, "At this stage of the litigation 'we presume[e] that these general allegations embrace those specific facts that are necessary to support' a link between [the plaintiff's injuries] and the data breaches." Id. Following SuperValu, Inc., this court concludes plaintiffs have clearly alleged the element of traceability.

C. Redressability

DMS does not challenge whether plaintiffs have sufficiently alleged standing's third element—redressability. In this court's opinion, plaintiffs have sufficiently alleged the three elements of standing as to their claims of past harm.

D. Standing to Seek Declaratory Judgment

DMS argues plaintiffs' claim for declaratory and injunctive relief should be dismissed for lack of standing because plaintiffs allege only an abstract future injury. Plaintiffs allege they will continue to face concrete substantial risks of future harm including fraud, identity theft, misuse of personal and private information, and cost of continuous credit monitoring because of DMS's failure to properly safeguard and prevent unauthorized disclosure of their private information.

Recently, another judge in this district considered a factually similar data breach case. Quaife v. Brady, Martz, & Assoc., P.C., No. 3:23-cv-176, 2024 WL 2319619 (D.N.D. May 22, 2024). In Quaife, a business discovered cybercriminals had accessed its information systems and databases and allegedly stole vast quantities of plaintiffs' private information. 2024 WL 2319619 at *1. The Quaife plaintiffs alleged they were at risk of harm due to the exposure of their private information and the defendant's failure to address the security failings that lead to that exposure. Id. at *6. The Quaife court determined, "At this early stage, there is an alleged risk of harm and injury in fact as to the stolen information that is sufficient to have standing to survive a motion to dismiss." Id. Based on Quaife, this court concludes plaintiffs have clearly alleged facts showing the elements of standing to survive a motion to dismiss the declaratory judgment claim.

2. Motion to Dismiss Under Rule 12(b)(6)

DMS also moves to dismiss plaintiffs' common law and statutory claims under Rule 12(b)(6), contending plaintiffs have failed to state any claim upon which relief could be granted. To state a claim upon which relief can be granted, a complaint must meet the requirements of Federal Rule of Civil Procedure 8(a)(2), as interpreted by Bell Atlantic Corp. v. Twombly, 550 U.S. 544 (2007), Ashcroft v. Iqbal, 556 U.S. 662 (2009),

and their progeny. To meet the Twombly/Iqbal standard, a complaint must present a "plausible" claim and must give the defendants fair notice of the claim and the grounds upon which it rests. E.g., Zink v. Lombardi, 783 F.3d 1089, 1098 (8th Cir. 2015). The plausibility standard requires "more than a sheer possibility that a defendant has acted unlawfully." Twombly, 550 U.S. at 557; Iqbal, 556 U.S. at 678. When the factual content of a complaint allows the court to reasonably infer a defendant is liable for the alleged misconduct, the complaint has stated a facially plausible claim. Iqbal, 556 U.S. at 678. In other words, the complaint must "possess enough heft to 'sho[w] that the pleader is entitled to relief.'" Twombly, 550 U.S. at 557 (quoting Fed. R. Civ. P. 8(a)(2)). While facts alleged in the complaint are to be accepted as true, conclusory allegations of the elements of a cause of action are insufficient to state a claim that is plausible on its face. Id.

Because this is a putative class action, with named plaintiffs who are residents of different states, "an individualized choice-of-law analysis must be applied to each plaintiff's claim." Quaife, 2024 WL 2319619 at *2 (quoting In re St. Jude Med., Inc., 425 F.3d 1116, 1120 (8th Cir. 2005)). In putative class actions, courts have generally declined to conduct a choice-of-law analysis prior to discovery because "the court does not have sufficient information to determine which state's law applies" and "it would be inappropriate to engage in an analysis of what state's laws are to be used throughout the remainder of the litigation." Cantonis v. Stryker Corp., 2011 WL 1084971, at *3 (D. Minn. Mar. 21, 2011).

As alleged in the amended complaint, DMS is a North Dakota corporation with its principal place of business in North Dakota, Boyd is a citizen of Minnesota, and Kolkind is a citizen of Texas. Boyd seeks to represent a Minnesota subclass and Kolkind

seeks to represent a Wisconsin subclass. A footnote in plaintiffs' responsive memorandum asserts Kolkind resided in Wisconsin for 22 years prior to relocation to Texas in August 2022. The footnote further asserts she provided the private information involved in this case while residing in Wisconsin and she continued to receive medical care in Wisconsin "as late as Spring 2023." (Doc. 46, p. 15 n.10).

Plaintiffs contend the court should apply North Dakota, Minnesota, and Wisconsin law to their claims. Id. But their responsive memorandum includes no analysis of their common law claims under Wisconsin law. DMS alleges the court should analyze the claims under North Dakota, Minnesota, and Texas law. The court will review plaintiffs' claims of negligence, breach of implied contract, breach of implied covenant of good faith and fair dealing, unjust enrichment, breach of a third-party beneficiary contract, and invasion of privacy claims under North Dakota, Minnesota, and Texas law. See Netgain Tech., 2022 WL 1810606, at *7.

A. Negligence Claim

Plaintiffs allege DMS's negligence resulted in a data breach. Though negligence claims are worded differently under the laws of North Dakota, Minnesota, and Texas, each state requires the plaintiff show the defendant owed the plaintiff a duty of care.[2] When determining if a duty exists under North Dakota law, the court considers the

[2] Under North Dakota law, to prevail on a negligence claim a plaintiff must prove (1) defendant owed a duty to the plaintiff, (2) defendant breached that duty, (3) plaintiff suffered an injury that was caused by the defendant, and (4) damages. Chegwidden v. Evenson, 863 N.W.2d 843, 848-49 (N.D. 2015). Under Minnesota law, to prevail on a negligence claim, a plaintiff must show (1) duty, (2) breach, (3) injury, and (4) a breach of duty was the proximate cause of the injury. Reichel v. Wendland Utz, LTD, 11 N.W.3d 602, 612 (Minn. 2024). To prevail on a negligence claim under Texas law, a plaintiff must show (1) a legal duty, (2) a breach of that duty, and (3) damages proximately caused by the breach. Gann v. Anheauser-Busch, Inc., 394 S.W. 83, 88 (Tex. App. 2012).

following factors: (1) foreseeability of harm to the plaintiff; (2) degree of certainty that the plaintiff suffered injury; (3) closeness of connection between the defendant's conduct and injury suffered; (4) moral blame attached to the defendant's conduct; (5) policy of preventing future harm; (6) extent of burden to the defendant and the consequences to the community of imposing a duty to exercise care with resulting liability for breach; and (7) availability, cost, and prevalence of insurance for the risk involved. Hurt v. Freeland, 589 N.W.2d 551, 555 (N.D. 1999). Minnesota general negligence law "imposes a general duty of reasonable care when the defendant's own conduct creates a foreseeable risk of injury to a foreseeable plaintiff. Domagala v. Rolland, 805 N.W.2d 14, 23 (Minn. 2011). A defendant can also owe a duty of care to a plaintiff "when action by someone other than the defendant creates a foreseeable risk of harm to the plaintiff and the defendant and plaintiff stand in a special relationship." Id.

Under Texas law, to determine if a duty exists, courts consider risk, foreseeability, likelihood of injury weighed against social utility of an actor's conduct, magnitude of the burden of guarding against the injury, and consequences of placing that burden on the actor. Bird v. W.C.W., 868 S.W.2d 767, 769 (Tex. 1994).

Plaintiffs allege DMS owed them a duty to act with reasonable care to secure and safeguard their private information. Plaintiffs allege DMS took on this obligation by storing plaintiffs' private information knowing that information was confidential and thus needed to be protected. Plaintiffs allege DMS knew or should have known the risks of storing private information, the vulnerabilities of its security system, and the importance of adequate data security. Plaintiffs allege DMS breached its duties to them by failing to provide adequate security systems to safeguard their private information and consequently allowing its network to be compromised by unauthorized parties.

Plaintiffs allege this breach led to the fraudulent use of their private information and to the risk of future misuse of their private information.

This court concludes the amended complaint contains sufficient factual allegations as to foreseeability, the connection between DMS and the unauthorized access to plaintiffs' private information, and injuries plaintiffs suffered as a result of their information being exposed to unauthorized access. This court finds plaintiffs have plausibly alleged DMS had a duty of care to safeguard their private information and therefore have plead sufficient facts to support the element of duty to proceed with their negligence claims under North Dakota, Minnesota, and Texas law.

Plaintiffs also allege DMS breached the duty it owed plaintiffs under the Health Insurance Portability and Accountability Act (HIPAA) by failing to adequately secure its data which caused the unauthorized disclosure of plaintiffs' PHI. Since HIPAA is a statute, plaintiffs' allegation that DMS violated a duty under HIPAA would be a negligence per se claim.

Plaintiffs allege DMS is a covered entity under HIPAA since it provides medical or health services to healthcare companies. Plaintiffs allege DMS breached its duties under HIPAA by allowing unauthorized access to their PHI by failing to implement proper security measures and safeguards. The HIPAA privacy rule prohibits the use or disclosure of individuals' PHI and requires covered entities to have security standards and safeguards to protect the privacy of PHI. 45 C.F.R. §§ 164.306, 164.308, 164.310, 164.312. 164.502. Covered entities include "health care provider[s] who transmit any health information in electronic form in connection with a transaction covered by this subchapter." 45 C.F.R. § 160.102(a)(3). Healthcare provider means "a provider of medical or health services" as defined in 42 U.S.C. § 1395x(s). 42 C.F.R. § 160.103.

"Medical and other health services" includes a multitude of services including imaging or x-ray services. 42 U.S.C. § 1395x(s)(3) and (4). "Protected health information" means individually identifiable health information. 42 C.F.R. § 160.103.

North Dakota does not recognize negligence per se claims. See Larson v. Kubisiak, 558 N.W.2d 852, 855 (N.D. 1997) (stating "the violation of a statutory duty is evidence of negligence and not negligence per se"). Under Minnesota law, "[n]egligence per se is a form of ordinary negligence that results from violation of a statute." Seim v. Haravalia, 306 N.W.2d 806, 810 (Minn. 1981). "A per se negligence rule substitutes a statutory standard of care for the ordinary prudent person standard of care, such that a violation of a statute . . . is conclusive evidence of duty and breach." Gradjelick v. Hance, 646 N.W.2d 225, 231 n.3 (Minn. 2002).

In Texas, to establish negligence per se, a plaintiff must prove the defendant's act, or omission violated a statute or ordinance, the injured person was in the class which the statute or ordinance was designed to protect, and the defendant's act or omission proximately caused the injury. Absher v. Zimmer, No. 04-12-00223-CV, 2012 WL 6029857, *1 (Tex. App. Dec. 5, 2012). But Texas federal courts have held HIPAA does not support a negligence per se claim because it does not provide for a private right of action, and it would therefore be against legislative intent to consider a violation of HIPAA to be negligence per se. See Smith v. Am. Pain & Wellness, PLLC, 747 F. Supp. 3d 989, 1004 (E.D. Tex. 2024); Walters v. Blue Cross & Blue Shield of Texas, Inc., No. 3:21-CV-981-L, 2022 WL 902735, at *5-6 (N.D. Tex. Mar. 28, 2022).

As to the duty element of a negligence claim, plaintiffs have alleged sufficient facts to support that element under North Dakota and Texas law, though neither North Dakota nor Texas would recognize a negligence per se claim. Plaintiffs have plead

sufficient facts to support a duty both under common law negligence and negligence per se claims under Minnesota law. As to other elements of a negligence claim, the court's analysis in section 1 applies. In this court's opinion, plaintiffs have pled a plausible negligence claim under North Dakota, Minnesota, and Texas law.

B. Breach of Implied Contract Claim

Plaintiffs allege DMS breached an implied contract. Under North Dakota, Minnesota, and Texas law, to state a claim for a breach of an implied contract, the plaintiff must show (1) the existence of a valid contract, (2) plaintiff's performance or tendered performance, (3) a breach of the contract, and (4) damages resulting from that breach. See Electrostim Med. Serv., Inc. v. Health Care Serv. Corp., 614 Fed App'x 731, 744 (5th Cir. 2015); Lord & Stevens, Inc. v. 3D Printing, Inc., 756 N.W.2d 789, 792-94 (N.D. 2008); Oehlerts & Sons Constr. v. Baustian, No. 67-CV-22-44, 2024 WL 4195163, *4 (Minn. Ct. App. Sept. 16, 2024); "An implied in fact contract is one the existence and terms of which are manifested by conduct. When dealing with contracts implied in fact the court is required to determine from the surrounding circumstances what the parties actually intended." Lord & Stevens, 756 N.W.2d at 793 (internal quotations omitted). An implied contract is deduced from the circumstances, relationships, and conduct of the parties. Oehlerts, 2024 WL 4195136, at *4. A valid implied contract can arise from acts and conduct of the parties. Harrison v. Williams Dental Grp., P.C., 140 S.W.3d 912, 916 (Tex. App. 2004). An implied "contract exists when the facts and circumstances surrounding the parties' relationship imply a mutual intention to contract. Every contract requires a meeting of the minds, but the meeting can be implied from and evidenced by the parties' conduct and course of dealing." Id.

Plaintiffs allege, through conduct, the parties entered into an implied contract for DMS to implement adequate data security measures to safeguard and protect plaintiffs' private information. Plaintiffs also allege they entered into a valid and enforceable implied contract with DMS when they first entered into a service agreement with DMS. Plaintiffs allege DMS required, solicited, and invited plaintiffs to entrust their private information as a condition of receiving DMS's services. Plaintiffs allege they accepted DMS's offers and provided their private information. Under the implied contracts, plaintiffs allege DMS promised and was obligated to provide imaging services to plaintiffs and protect plaintiffs' private information. In exchange, plaintiffs allege they agreed to pay money for those services. Those provisions were acknowledged, memorialized, and embodied in multiple documents, including DMS's privacy notice and notification letter. Plaintiffs allege DMS breached the implied contracts when it failed to safeguard and protect their private information. Plaintiffs allege the damages include increased risks of identity theft.

This court finds plaintiffs have plausibly alleged the existence of an implied contract as well as its terms, and these allegations are sufficient to allow the claim to go forward under North Dakota, Minnesota, and Texas law.

C. Breach of Implied Covenant of Good Faith and Fair Dealing Claim

Plaintiffs allege DMS breached the implied covenant of good faith and fair dealing by failing to maintain data security adequate to safeguard plaintiffs' private information, failing to timely and accurately disclose the data breach, and continuing to accept and store private information after DMS knew or should have known about its security vulnerabilities. Plaintiffs allege, "Every contract in this State has an implied

covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms." [3] (Doc. 36, p. 31).

North Dakota has recognized the doctrine of an implied covenant of good faith and fair dealing only as it relates to insurance contracts. Dalan v. Paracelsus Healthcare Corp. of N.D., 640 N.W.2d 726, 731 (N.D. 2002). The claim is more widely recognized under Minnesota law, where "every contract includes an implied covenant of good faith and fair dealing requiring that one party not 'unjustifiably hinder' the other party's performance of the contract." In re Hennepin Cnty. 1986 Recycling Bond Litig., 540 N.W.2d 494, 502 (Minn. 1995). Under Texas law, not all contracts include an implied covenant of good faith and fair dealing. Subaru of Am., Inc. v. David McDavid Nissan, Inc., 84 S.W.3d 212, 225 (Tex. 2002). A covenant of good faith and fair dealing arises under Texas law only when a contract creates or governs a special relationship between the parties, like that between an insurer and insured. Id.; Dallas/Fort Worth Int'l Airport Bd. v. Vizant Tech., 576 S.W.3d 362, 369 n.13 (Tex. 2019).

This court concludes plaintiffs' allegations do not support a claim of breach of an implied covenant of good faith and fair dealing under North Dakota law, since there are no allegations related to an insurance contract. Although plaintiffs allege DMS failed to fulfill a contractual duty, they do not allege DMS unjustifiably hindered contract performance and thus fail to state a claim under Minnesota law. Additionally, there is no allegation DMS and the plaintiffs had a special relationship, like insurer and insured, to state a claim under Texas law. Therefore, the amended complaint does not plausibly

[3] The amended complaint does not identify the state to which this allegation refers.

allege a breach of an implied covenant of good faith and fair dealing, and the claim will be dismissed.

D. Unjust Enrichment Claim

Plaintiffs claim DMS was unjustly enriched. Under North Dakota law,

> Unjust enrichment is a broad, equitable doctrine which rests upon quasi or constructive contracts implied by law to prevent a person from unjustly enriching himself at the expense of another. To recover under a theory of unjust enrichment, the plaintiff must prove: (1) an enrichment, (2) an impoverishment, (3) a connection between the enrichment and the impoverishment, (4) the absence of a justification for the enrichment and impoverishment, and (5) the absence of a remedy provided by law. The theory may be invoked when a person has and retains money or benefits which in justice and equity belong to another. For a complainant to recover, it is sufficient if another has, without justification, obtained a benefit at the direct expense of the complainant, who then has no legal means of retrieving it. The essential element in recovering under the theory is the receipt of a benefit by the defendant from the plaintiff which would be inequitable to retain without paying for its value.

McDougall v. AgCountry Farm Credit Servs., PCA, 937 N.W.2d 546, 553 (N.D. 2020). "The essential element in recovering under the theory is the receipt of a benefit by the defendant from the plaintiff. . . ." Thimjon Farms P'ship v. First Int'l Bank & Tr., 837 N.W.2d 327, 336 (N.D. 2013) (emphasis added).

Under Minnesota law, "To establish an unjust enrichment claim it must be shown that a party has knowingly received something of value, not being entitled to the benefit, and under circumstances that would make it unjust to permit its retention." Southtown Plumbing, Inc. v. Har-Ned Lumber Co., Inc., 493 N.W.2d 137, 140 (Minn. Ct. App. 1992). "Minnesota also requires a direct relationship between the parties and no other available remedy in a claim for unjust enrichment." Quaife, 2024 WL 2319619, at *4; see also Southtown, 493 N.W.2d at 140.

Under Texas law, "Unjust enrichment occurs when a person has wrongfully secured a benefit or has passively received one which it would be unconscionable to retain. A person is unjustly enriched when he obtains a benefit from another by fraud, duress, or the taking of an undue advantage." Eun Bok Lee v. Ho Chang Lee, 411 S.W.3d 95, 111 (Tex. App. 2013) (emphasis added).

Plaintiffs allege they entrusted their private information to DMS for the purpose of obtaining healthcare services and reasonably believed DMS would keep their private information secure. Plaintiffs allege DMS received enrichments such as profits, benefits, and other compensation by failing to invest in reasonable security measures to protect its private information.

DMS argues plaintiffs must allege a direct relationship between DMS and plaintiffs to plausibly plead an unjust enrichment claim. Further, DMS cites SuperValu, Inc. for the proposition that plaintiffs must allege they "paid a premium" to DMS for protection of their private information. (Doc. 42, p. 19).

But plaintiffs argue lack of a direct relationship would not in itself preclude an unjust enrichment claim, citing McDougall v. AgCountry Farm Credit Services., 960 N.W.2d 792 (N.D. 2020).[4] McDougall held that a third party having "participated somehow in the transaction through which the benefit is obtained" is a fact the court must consider in determining whether there is a causal connection between the impoverishment and the enrichment. Id. at 799. But the facts of McDougall are quite different from those of this case.

[4] In plaintiffs' opposition brief, they cite to McDougall v. AgCountry Farm Credit Servs., PCA, 937 N.W.2d 546, 553 (N.D. 2020) and McDougall v. AgCountry Farm Credit Servs., 960 N.W.2d 792 (N.D. 2021) interchangeably. (Doc. 46, p. 21).

In McDougall, the defendant had made representations to non-party mortgagees that "additional collateral would assist in moving refinancing forward," knowing the conversation would be relayed to the plaintiffs. Id. at 795. The defendant's representations led the plaintiffs to transfer land to the mortgagees, but despite that additional collateral, the defendant denied the mortgagees' refinancing application. The plaintiffs would not have transferred the land if they had known the mortgagees' refinancing application would be denied.

Recently, the Quaife court determined a plausible unjust enrichment claim must be supported by an allegation of a direct relationship between the plaintiffs and the defendants. 2024 WL 2319619, at *4. The Quaife court held, "Here there is no allegation of a direct relationship between the Plaintiffs and [the defendant]. Nor could there be. There was no benefit conferred to [the defendant] by the Plaintiffs because [the defendant] did not contract with the Plaintiffs . . . it contracted with the Plaintiffs' employers." Id. The case at hand is similar, there are no allegations of a direct relationship between plaintiffs and DMS, nor could there be, because the allegations are that DMS directly contracted with plaintiffs' healthcare providers, not with plaintiffs.

Minnesota law does not support plaintiff's unjust enrichment claim. This court concludes plaintiffs' allegations are insufficient under McDougall to plausibly allege an unjust enrichment claim, and the claim will be dismissed under North Dakota Law. Nor have plaintiffs plausibly alleged the fraud, duress, or taking unfair advantage required under Texas law.

E. Breach of Third-Party Beneficiary Contract Claim

Plaintiffs claim a breach of a third-party beneficiary contract. North Dakota law provides a contract made expressly for the benefit of a third party may be enforced at

any time; to enforce a contract between two other parties, the contracting parties must have intended a third party be benefited by the contract. If a third party's benefit was purely incidental and not contemplated by the contracting parties, the third party cannot sue to enforce the contract. Apache Corp. v. MDU Res. Grp., Inc., 603 N.W.2d 891, 894; Peoples State Bank of Truman, Inc. v. Molstad Excavating, Inc., 721 N.W.2d 43, 48 (N.D. 2006).

Under Minnesota law, a third party can assert rights under a contract if the third party was an intended beneficiary of the contract. A person is an intended beneficiary if

> (1) the beneficiary's right to performance reflects the intent of the parties to the contract; and (2) performance of the contract "satisf[ies] an obligation of the promisee to pay money to the beneficiary [the duty owed test]; or . . . the circumstances indicate that the promisee intends to give the beneficiary the benefit of the promised performance [intent-to-benefit test]. . . . [I]f recognition of third-party rights is "appropriate" and either the duty owed test or the intent to benefit test is met, the third party can recover as an "intended beneficiary."

Minn. Laborers Health & Welfare Fund v. Granite RE, Inc., 826 N.W.2d 210, 214 (Minn. 2012); see also Hickman v. Safeco Ins. Co. of Am., 695 N.W.2d 365, 369 (Minn. 2005).

Texas law states "[a] third party may recover on a contract made between other parties only if the parties intended to secure some benefit to that third party, and only if the contracting parties entered into the contract directly for the third party's benefit." MCI Telecomms. Corp. v. Tex. Util. Elec. Co., 995 S.W.2d 647, 651 (Tex. 1999).

Plaintiffs allege DMS and their healthcare providers contracted to provide imaging services to plaintiffs. Plaintiffs allege the contracts included DMS's promises to provide data retention and security services to protect private information in compliance with data protection statutes and industry standards. Plaintiffs allege they became third-party beneficiaries once their healthcare providers gave their information

to DMS and allege DMS breached the contract by failing to deliver reasonable data security measures to protect plaintiffs' private information. DMS alleges plaintiffs fall short of establishing there was a contract between DMS and plaintiffs' healthcare providers and that plaintiffs were indeed intended beneficiaries of that contract. DMS states plaintiffs' "claims are entirely speculative assumptions of the Plaintiffs, as they do not have access to these alleged contracts between DMS and their 'clients.'" (Doc. 42, p. 22).

Plaintiffs have alleged sufficient facts to support their claim that they were intended third-party beneficiaries under North Dakota, Minnesota, and Texas law and the contracts under which they were third-party beneficiaries were breached. Therefore, the amended complaint plausibly alleges a breach of a third-party beneficiary contract.

F. Invasion of Privacy Claim

Plaintiffs claim DMS invaded their privacy. North Dakota courts have not recognized a tort action for invasion of privacy. Hogum v. Valley Mem'l Homes, 574 N.W.2d 812 (N.D. 1998). In Hogum, the court relied on requirements of intrusion upon seclusion under the Second Restatement of Torts in addressing whether to recognize an invasion of privacy claim. "A claim for intrusion upon seclusion requires (1) an intentional intrusion by the defendant, (2) into a matter the plaintiff has a right to keep private, (3) which is objectionable to a reasonable person." Hogum, 574 N.W.2d at 816-17; see also Restatement (Second) of Torts § 652B. "Generally, there are two primary factors for analyzing a claim for intrusion upon seclusion: (1) the means used for the intrusion, and (2) the defendant's purpose for obtaining the information." Hogum, 574 N.W.2d at 817.

"Minnesota recognizes the tort of invasion of privacy on three alternative theories: intrusion of seclusion, appropriation of a name or likeness of another, and publication of private facts." Yath v. Fairview Clinics, N.P., 767 N.W.2d 34, 42 (Minn. Ct. App. 2009). "There are three elements of the tort of intrusion upon seclusion: "(a) an intrusion; (b) that is highly offensive; (c) into some matter in which a person has a legitimate expectation of privacy." Jones v. Walgreens Co., No. A11-1261, 2012 WL 1658895, at *4 (Minn. Ct. App. May 14, 2012).

Texas courts have held, "To establish an actionable invasion of privacy of the type the [plaintiffs] allege—intrusion-upon-seclusion—a plaintiff must show (1) an intentional intrusion, physically or otherwise, upon another's solitude, seclusion, or private affairs or concerns, which (2) would be highly offensive to a reasonable person. Moore v. Bushman, 559 S.W.3d 645, 649 (Tex. App. 2018).

Plaintiffs allege they provided and entrusted DMS with their private information. Plaintiffs allege DMS failed to protect their private information and thereby allowed unauthorized unknown parties to access their private information. Plaintiffs allege the unauthorized release of their private information is highly offensive to a reasonable person. Plaintiffs allege the intrusion involved information that was meant to stay private. Plaintiffs allege the breach at the hands of DMS creates an intentional intrusion.

But plaintiffs do not allege DMS intruded into their private information. In fact, plaintiffs allege the opposite. Plaintiffs allege they gave their private information to DMS, thus not alleging an intrusion by DMS. DMS cites to a federal district court case that recently addressed this issue. See Linman v. Marten Transp., 2023 WL 2562712 (W.D. Wis. 2023) (applying Wisconsin law). The court in Linman determined the plaintiff did not state a claim for intrusion

upon seclusion because it was hackers, not the defendants that intruded on the plaintiff's privacy. Because the plaintiff provided his personal information to the defendants willingly, the defendants did not intrude on the plaintiff's privacy by collecting it. "The only 'intrusion' was the alleged breach by the hackers." Id. at *6. This court concludes the amended complaint does not plausibly allege breach of invasion of privacy by DMS under North Dakota, Minnesota, or Texas law, and the claim will be dismissed.

G. Claim Under North Dakota Century Code Section 51-22-02

Plaintiffs claim DMS violated North Dakota Century Code section 51-22-02, which states,

> No business entity which charges a fee for data processing services performed may disclose in whole or in part the contents of any record, including the disclosure of information contained in the record through inclusion in any composite of information, which is prepared or maintained by such business entity to any person, other than the individual or business entity which is the subject of the record, without the express written consent of such individual or business entity.

Plaintiffs allege DMS is a business entity under section 51-22-02 because DMS's principal place of business is North Dakota. Plaintiffs also allege DMS charges a fee for data processing services, defined as "any systematic sequence[s] of operations, including but not limited to bookkeeping functions, inventory control, storage, or manipulation and retrieval of management or personnel information." N.D. Cent. Code § 51-22-01. Plaintiffs allege DMS disclosed their private information to third parties without their consent by failing to take appropriate measures to safeguard their private information.

DMS relies on Quaife to support dismissal of the claim of violation of section 51-22-02. Since section 51-22-02 does not define the word "disclosure," the Quaife court utilized the definition of "disclose" or "disclosure" from North Dakota Century Code

section 32-49-01 (3), as allowed under North Dakota Century Code section 1-01-09. Per section 32-49-01 (3), "disclose" means to transfer, publish, or distribute to another person. The Quaife court held disclosure requires some type of action, but what the plaintiffs alleged was inaction, therefore plaintiffs' allegation of the defendant's inaction was not enough to plausibly allege a claim under section 51-22-02.

In their opposition to the motion to dismiss, plaintiffs argue the Quaife court's analysis as it relates to section 51-22-02 was limited to whether a data breach resulting from "inaction" can constitute a statutory violation. In contrast, plaintiffs here argue they allege more than an "inaction" by DMS, plaintiffs argue they allege "[d]efendant's data security practices fell short of reasonable standards. By failing to employ adequate security measures despite knowing the cybersecurity DMS effectively enabled unauthorized third-party access." (Doc. 46, p. 17).

Yet, plaintiffs' arguments are nearly identical to what the plaintiffs alleged in Quaife,

> Defendant disclosed Plaintiffs and Class Member's PI to third parties without their consent by failing to take appropriate measures to safeguard and protect the PI amidst foreseeable risk of a cybersecurity attack, resulting in a Data Breach.

2024 WL 2319619 at *5. This court agrees with the analysis in Quaife and concludes plaintiffs have not plausibly alleged that DMS disclosed plaintiffs' private information in violation of North Dakota Century Code section 51-22-02, and the claim will be dismissed.

Conclusion

This court finds plaintiffs have sufficiently alleged standing. Insofar as DMS moves to dismiss under Rule 12(b)(1), the motion is **DENIED**. Additionally, after

applying Rule 12(b)(6) standards to the amended complaint, DMS's motion to dismiss the amended complaint, (Doc. 36), is **GRANTED IN PART** and **DENIED IN PART**. The claims of breach of an implied covenant of good faith and fair dealing, invasion of privacy, unjust enrichment, and violation of North Dakota Century Code section 51-22-02 are **DISMISSED**. Plaintiffs may proceed on the claims of negligence, breach of implied contract, and breach of a third-party beneficiary contract.

IT IS SO ORDERED

Dated this 8th day of July, 2025.

/s/ Alice R. Senechal
Alice R. Senechal
United States Magistrate Judge